Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended)

Claim 2 (currently amended)

Claim 3 (currently amended)

Claim 4 (currently amended)

Claim 5 (currently amended)

Claim 6 (currently amended)

Claim 7 (currently amended)

Claim 8 (currently amended)

Claim 9 (currently amended)

Claim 10 (currently amended)

Claim 11 (currently amended)

Claim 12 (original)

Claim 13 (currently amended)

Claim 14 (currently amended)

Claim 15 (currently amended)

Claim 16 (currently amended)

Claim 17 (currently amended)

claim 18 (currently amended)

Claim 19 (currently amended)

Claim 20 (currently amended)

Claim 21 (currently amended)

Claim 22 (currently amended)

Claim 23 (currently amended)

Claim 24 (original)

Claim 25 (currently amended)

1. (Currently amended)

A method of creating certificates with redundant information to certify several keys, wherein each of the certificates comprises a defined number of data elements which at least contain information on the a certification body (issuer of the certificate), the a user of the certificate and the a key certified by the certificate, characterized by the following steps:

a) Specification specification of a request for certification of one or more of several keys by [[a]] the certification body for [[a]] the user[[.]] ;

b) [[If]] if in step a) only one key is to be initially certified, and no basic certificate is yet available for the user, creation of a basic certificate for the user with a defined number of data elements which, in the certification process, are identical for the respective user in conjunction with the respective certification body[[.]] ;

c) Addition addition of an identifying characteristic to the basic certificate[[.]] ;

d) Generation generation of a digital signature for the basic certificate[[.]] ;

e) Addition addition of the digital signature to the basic certificate[[.]] ;

f) Generation generation of a key pair[[.]] ;

g) ~~Creation~~ creation of a supplementary certificate for the basic certificate with a key as set out in step f), the identifying characteristic as set out in step c) and additional data fields not registered by the basic certificate[[.]] ;

h) ~~Generation~~ generation of a digital signature for the supplementary certificate[[.]] ;

i) ~~Addition~~ addition of the digital signature to the supplementary certificate[[.]] ;

j) ~~Use~~ use of an existing basic certificate for the only one key when the one key shares the redundant information with the existing basic certificates[[.]] ; and

k) ~~Use~~ use of the basic certificate created in step b) for future keys that share the redundant information with the basic certificate.

2. (Currently amended)

The method in accordance with Claim 1, characterized in that the basic certificate comprises the following data elements:

- ~~Name~~ name of the certification body,

- ~~User~~ user ID of the certification body,

- ~~Name~~ name of the user,

- ~~User~~ user ID of the user, and

- ~~Identifying~~ identifying characteristic of the basic certificate.

3. (Currently amended)

The method in accordance with Claim 1, characterized in that the supplementary certificate comprises the following data elements:

- ~~Signature~~ a signature algorithm,

- ~~Key~~ a key,

- ~~Serial~~ serial number of the key,

- ~~Validity~~ a validity period of the certificate,

- ~~Extensions~~ extensions, and

- ~~Identifying~~ an identifying characteristic of the basic certificate.

4. (Currently amended)

The method in accordance with Claim 1, characterized in that if step a) reveals that more than one key with the same validity period is to be certified at one time, instead of steps b) - i) the following steps are executed:

aa) ~~Generation~~ generation of several key pairs[[.]] ;

bb) ~~Generation~~ generation of a single group certificate (group certificate) for the several keys with all data elements necessary for the individual keys and keys generated in step aa), with only a single recitation of data elements redundant to all the several keys in the group certificate[[.]] ;

cc) ~~Generation~~ generation of a digital signature for the group certificate[[.]] ; and

dd) ~~Addition~~ addition of the digital signature to the group certificate.

5. (Currently amended)

The method in accordance with Claim 4, characterized in that the <u>basic</u> certificate contains the following data elements:

- ~~Name~~ <u>name</u> of <u>the</u> certification body<u>,</u>

- ~~User~~ <u>user</u> ID of <u>the</u> certification body<u>,</u>

- ~~Name~~ <u>name</u> of <u>the</u> user<u>;</u>

- ~~User~~ <u>user</u> ID of user<u>;</u>

- ~~Type/version~~ <u>type/version</u> of the certificate<u>,</u>

- ~~Number~~ <u>number</u> and types of keys<u>,</u>

- ~~Key~~ <u>a key,</u>

- ~~Validity~~ <u>validity,</u>

- ~~Serial~~ <u>serial</u> number<u>, and</u>

- ~~Extensions~~ <u>extensions.</u>

6. (Currently amended)

The method in accordance with Claim 1 characterized in that, if only one key is to be certified in step a) and a basic certificate already exists as stated in step j) or k), instead of steps b) - i) the following steps are executed:

aa)   ~~Definition~~ <u>definition</u> of the basic certificate and reading of the identifying characteristics of the basic certificate[[.]] <u>;</u>

bb)   ~~Generation~~ <u>generation</u> of a key pair[[.]] <u>;</u>

cc)   ~~Creation~~ <u>creation</u> of a supplementary certificate for the basic certificate with additional data fields not registered by the basic certificate, wherein one of the keys is inserted into the supplementary certificate in step bb)[[.]] <u>;</u>

dd)   ~~Insertion~~ <u>insertion</u> of the identifying characteristics in accordance with step aa) into the supplementary certificate to locate the associated basic certificate[[.]] <u>;</u>

ee)   ~~Generation~~ <u>generation</u> of a digital signature for the supplementary certificate[[.]] <u>; and</u>

ff)   ~~Addition~~ <u>addition</u> of the digital signature to the supplementary certificate.

7. (Currently amended)

The method in accordance with Claim 6, characterized in that ~~the~~ <u>any</u> supplementary certificates each contain the following data elements:

- ~~Signature~~ <u>a signature</u> algorithm<u>,</u>

- ~~Key~~ <u>a key,</u>

- ~~Serial~~ <u>serial</u> number of <u>the</u> key<u>,</u>

- ~~Validity~~ <u>validity</u> period of the certificate<u>,</u>

- ~~Extensions~~ <u>extensions, and</u>

- ~~Identifying~~ <u>identifying</u> characteristic of the basic certificate<u>.</u>

8. (Currently amended)

The method for creating a certificate for simultaneous certification of several keys with the same validity period, wherein the certificate comprises a defined number of data elements which at least contain information on the certification body (issuer of the certificate), the user of the certificate and the key certified by the certificate, characterized by the following steps:

aa)   ~~Generation~~ generation of several key pairs[[.]] ;

bb)   ~~Generation~~ generation of a single joint or group certificate (group certificate) for several keys with all data elements necessary for the individual keys and keys generated in step aa), with the group certificate containing only a single recitation of data elements[[.]] ;

cc)   ~~Generation~~ generation of a digital signature for the group certificate[[.]] ; and

dd)   ~~Addition~~ addition of the digital signature to the group certificate.

9. (Currently amended)

The method in accordance with Claim 8, characterized in that the group certificate contains the following data elements:

- ~~Name~~ name of the certification body,

- ~~User~~ user ID of the certification body,

- ~~Name~~ name of the user,

- ~~User~~ user ID of <u>the</u> user,

- ~~Type/version~~ <u>type/version</u> of the <u>group</u> certificate,

- ~~Number~~ <u>number</u> and types of keys,

- ~~Key~~ <u>key,</u>

- ~~Validity~~ <u>validity,</u>

- ~~Serial~~ <u>serial</u> number<u>, and</u>

- ~~Extensions~~ <u>extensions.</u>

10. (Currently amended)

A method for creating a certificate for certification of a new key for a user, wherein the certificate comprises a defined number of data elements which at least contain information on ~~the~~ <u>a</u> certification body (issuer of the certificate), ~~the~~ <u>a</u> user of the certificate and the key certified by the certificate, wherein a basic certificate for the user already exists and the basic certificate comprises data elements which, in the certification process, are identical for the respective user in conjunction with the respective certification body, characterized by the following steps:

aa) ~~Definition~~ <u>definition</u> of the basic certificate for the user and reading of the identifying characteristics of the basic certificate[[.]] <u>;</u>

bb) ~~Generation~~ <u>generation</u> of a key pair for the new key[[.]] <u>;</u>

cc) ~~Creation~~ <u>creation</u> of a supplementary certificate for the basic certificate with additional data fields not registered by the basic certificate, wherein one of the keys <u>of the key pair generated in step bb</u> is inserted into the supplementary certificate ~~in step bb).~~ <u>;</u>

dd)   ~~Insertion~~ insertion of the identifying characteristics in accordance with step aa) into the supplementary certificate to locate the associated basic certificate[[.]] ;

ee)   ~~Generation~~ generation of a digital signature for the supplementary certificate[[.]] ; and

ff)   ~~Addition~~ addition of the digital signature to the supplementary certificate.

11. (Currently amended)

The method in accordance with Claim 10, characterized in that the supplementary certificate contains the following data elements:

- ~~Signature~~ a signature algorithm,
- ~~Key~~ a key,
- ~~Serial~~ serial number of the key,
- ~~Validity~~ validity period of the certificate,
- ~~Extensions~~ extensions,
- ~~Identifying~~ an identifying characteristic of the basic certificate.

12. (Original)

The method in accordance with Claim 8, characterized in that the key is a public key.

13. (Currently amended)

The method in accordance with Claim 1, characterized in that the basic certificate and the supplementary certificate are stored in ~~the~~ a non-volatile memory of a chipcard.

14. (Currently Amended)

The method in accordance with Claim 4, characterized in that the <u>basic</u> certificate (group certificate) is stored in ~~the~~ a non- volatile memory of a chipcard.

15. (Currently amended)

The method for reading certificates created in accordance with Claim 1, characterized by the following steps:

a)   ~~Cheek~~ <u>check</u> of the storage medium for presence of basic certificates[[.]] ;

b)   ~~If~~ <u>if a basic certificate is</u> present, identification of the necessary supplementary certificate[[.]] ;

c)   ~~Read-in~~ <u>reading-in</u> of the supplementary certificate ~~to~~ <u>into</u> the RAM of a system[[.]] ;

d)   ~~Definition~~ <u>definition</u> of the identification number of the basic certificate from the supplementary certificate[[.]] ; and

e)   ~~Read-in~~ <u>reading-in</u> of the basic certificate ~~to~~ <u>into</u> the RAM.

16. (Currently amended)

The method in accordance with Claim 15, characterized in that, if no basic certificate could be identified in step a), instead of steps b) - e) the following steps are executed:

f)   ~~Check~~ check of the storage medium for presence of group certificates[[.]] ; and

g)   ~~Read-in~~ reading-in of ~~the~~ a necessary group certificate[[s]] ~~to~~ into the RAM.

17. (Currently amended)

The method for reading of certificates created in accordance with Claim 10, characterized by the following steps:

a)   ~~Check~~ check of the storage medium for presence of group certificates[[.]] ; and

b)   ~~Read-in~~ reading-in of ~~the~~ a necessary group certificate ~~to~~ into the RAM.

18. (Currently amended)

The method in accordance with Claim 17, characterized in that the storage medium is a non-volatile memory of ~~the~~ a chipcard.

19. (Currently amended)

A computer program product on a computer usable medium for creating [[a]] certificates to certify several keys sharing redundant information, wherein ~~the~~ a certificate comprises a defined number of data elements which at least contain information on the certification body (issuer to the certificate), the user of the certificate and the key certified by the certificate, said computer program product comprising:

a) software for specification of a request for certification of <u>at least</u> one of the several keys by a certification body for a user;

b) software for creation of a basic certificate for the user with a defined number of data elements which, in the certification process, are identical for the respective user in conjunction with the respective certification body when initially only one key is to be certified, and no basic certificate is yet available for the user;

c) software for the addition of an identifying characteristic to the basic certificate;

d) software for the generation of a digital signature for the basic certificate;

e) software for the addition of the digital signature to the basic certificate;

f) software for generation of a key pair;

g)   software for creation of a supplementary certificate for the basic certificate with a key as set out in f), the identifying characteristic as set out in c) and additional data fields not registered by the basic certificate;

h)   software for generation of a digital signature for the supplementary certificate;

i)   software for addition of the digital signature to the supplementary certificate; and

j)   use of the basic certificate created in step b) with future keys that share the redundant information with the basic certificate by issuing an additional supplementary certificate with a new key pair.

20. (Currently amended)

The computer program product in accordance with Claim 19, characterized in that the basic certificate comprises the following data elements:

-      ~~Name~~ name of the certification body,

-      ~~User~~ user ID of the certification body,

-      ~~Name~~ name of the user,

-      ~~User~~ user ID of the user, and

-      ~~Identifying~~ identifying characteristic of the basic certificate.

21. (Currently amended)

The computer program product in accordance with Claim 19, characterized in that the supplementary certificates comprise the following data elements:

- ~~Signature~~ a signature algorithm,
- ~~Key~~ a key,
- ~~Serial~~ a serial number of the key,
- ~~Validity~~ a validity period of the certificate,
- ~~Extensions~~ extensions, and
- ~~Identifying~~ identifying characteristic of the basic certificate.

22. (Currently amended)

The computer program product in accordance with Claim 19, characterized in that if more than one key with the same validity period is to be certified at one time, the following software replaces the software of b) to i)[[;]] :

aa)   software for generation of several key pairs;

bb)   software for generation of a certificate (group certificate) for several keys with all data elements necessary for the individual keys and keys generated in step aa), omitting the redundant data elements;

cc)   software for generation of a digital signature for the certificate; and

dd)   software for addition of the digital signature to the certificate.

23. (Currently amended)

The computer program product software in accordance with Claim 22, characterized in that the <u>group</u> certificate contains the following data elements:

- ~~Name~~ <u>name</u> of <u>the</u> certification body,
- ~~User~~ <u>user</u> ID of <u>the</u> certification body,
- ~~Name~~ <u>name</u> of <u>the</u> user,
- ~~User~~ <u>user</u> ID of <u>the</u> user,
- ~~Type/version~~ <u>type/version</u> of the certificate,
- ~~Number~~ <u>number</u> and types of keys,
- ~~Key~~ <u>a key,</u>
- ~~Validity~~ <u>validity,</u>
- ~~Serial~~ <u>serial</u> Number, <u>and</u>
- ~~Extensions.~~ <u>extensions.</u>

24. (Original)

The computer program product in accordance with Claim 19, characterized in that, if only one key is to be certified and a basic certificate already exists, the following software replaces the software of b) to i):

aa)   software code definition of the basic certificate and reading of the identifying characteristics of the basic certificate;

bb)   software code for generation of a key pair;

cc)   software code for creation of a supplementary certificate for the basic certificate with additional data fields not registered by the basic certificate, wherein one of the keys is inserted into the supplementary certificate by step bb);

dd)   software code insertion of the identifying characteristics in accordance with step aa) into the supplementary certificate to locate the associated basic certificate;

ee)   software code generation of a digital signature for the supplementary certificate; and

ff)   software code addition of the digital signature to the supplementary certificate.

25. (Currently amended)

The computer program product in accordance with Claim 24, characterized in that the supplementary certificate contains the following data elements:

-     ~~Signature~~ a signature algorithm,
-     ~~Key~~ a key,
-     ~~Serial~~ serial number of the key,
-     ~~Validity~~ validity period of the supplementary certificate,
-     ~~Extensions~~ extensions, and
-     ~~Identifying~~ identifying characteristic of the basic certificate.